WORKING THREAD: 702 MINIMIZATION PROCEDURES (FBI)

FBI

(2) Does the exclusion of data acquired with consent incorporate the Third Party doctrine assumption that you've given your metadata over willingly? Because the FBI is using 702 acquired data for metadata analysis.

(2) The definitions of who is and who is not a USP are very very permissive. That's because being outside the US or "not known" is presumptively a non-USP — but we know they claim not to track location that closely. So it's presumably very easy for them to not know and keep tracking a USP. Moreover, the IOB and 702 IG report show that the FBI doesn't necessarily double check NSA data on location, so they may not learn even if NSA has subsequently learned someone is a USP.

(3) How many contractors are included in this definition of FBI personnel? And do they include "contractors" who troll chat rooms for potential targets?

(3) This states the procedures should not limit lawful oversight of among other things, the appropriate IGs. So why is DOJ IG having such a hard time tracking things like this?

(3-4) FBI can keep 702 data for up to a year to conduct security assessments of its own systems. Why would 702 data be targeted like that?

(4) This section appears to be the directly acquired data—so why is ODNI still redacting the description of it?

(4) What does FBI mean by "end user" among those who have to delete data that has been improperly collected? Does it include data handed onto localities?

(5) Note the specific permission for multiple users accessing information simultaneously "or sequentially" and sharing back and forth. What's that about? Also, I'm struck by the absence of any requirement on login credentials, as NSA procedures often include. Is it possible FBI only audits this via log? And how is the log generated?

(5) Note the SMPs specifically include photos among FISA data.

(6) As with the NSA, the FBI is permitted to keep data that has been determined to be USP data if it is information "retained for cryptanalytic, traffic analytic, or signal exploitation process." While this determination is supposed to happen on a communication-by-communication basis (which should work out to be more restrictive than NSA), it also broadly permits FBI to keep anything encrypted, even if it's USP data collected domestically.

(7) If people "assisting in a lawful and authorized governmental function" are not doing it as part of their job duties, it seems to suggest sharing outside of professionals. Again, that could include broadly defined "consultants."

(7) The audit language appears to require only audits of people who've accessed raw data, not what they've done while accessing it.

(7-8) This language appears to permit the FBI to retroactively reclassify something FI data. This permissiveness would seem to breed permanent retention.

(8) Those getting 702 data aren't apparently required to go through training; they're just informed the SMPs exist. This is one of a number of ways that FBI's SMPs are more lenient than NSA's, precisely on information sharing.

(8) What does this mean, legally? "Such personnel shall exercise reasonable judgment in making such determinations" [about whether something is foreign intelligence, important, or

evidence of a crime]?

(9) The footnote on metadata is key: the FBI case managers don't have to identify whether metadata has been disseminated, nor that it has met retention standards. This means the standards on PRISM-acquired metadata are vastly more lenient than they were under the PRTT program.

(10) SMPs use the passive voice when instructing people "particular care should be taken" when reviewing sensitive information. A classic rule in procedures writing is if you don't intend the procedures to work, write them in the passive voice.

> Information that reasonable appears to be foreign intelligence information, necessary to understand foreign intelligence information, or necessary to assess the importance of foreign intelligence information may be retained, processed, and disseminated in accordance with these procedures even if it is sensitive information.

(11) I'm wondering if the redaction talks about how those not authorized to access this data can get others to do so for them (as was indicated in PCLOB).

(11) This is interesting. After saying that queries need to be tracked (see above for my concern about whether these queries are audited), it says this:

> For purposes of this section, the term query does not include a user's search or query of an FBI electronic and data storage system that contains raw FISA-acquired information, where the user does not receive the raw FISA-acquired information in response to the search or query or otherwise have access to the raw FISA-acquired information that is searched.

This seems to suggest, first of all, that if someone queries data they shouldn't, no record will be kept. But also recall my suspicions about how defeat lists work, including that informants would be defeated from a lot of kinds of searches. That means (if my guess is correct) that FBI would never be held accountable for researching on one of their informants but getting no return. Consider how this would work if, for example, Tam Tsarnaev was informing for FBI, as some evidence suggests he was.

(11) More on the permissions involving metadata:

> Users authorized to access FBI electronic and data storage systems that contain "metadata" may query such systems to find, extract, and analyze "metadata" pertaining to communications. The FBI may also use such metadata to analyze communications and may upload or transfer some or all such metadata to other FBI electronic and data storage systems for authorized foreign intelligence or law enforcement purposes. For purposes of these procedures, "metadata" is dialing, routing, addressing, or signaling information associated with a communication, but does not include information concerning the substance, purport, or meaning of the communication.

Bet you $100 there's a juicy FISC opinion on this. Note, especially, that FBI clearly has access to stuff that is metadata but that has nothing to do with a communication. These SMPs already told us they're also getting photos. They also don't comment, one way or another, about location.

(12) As with NSA under 12333 but not their old 702 SMPs, FBI has to consult with GC on whether something is privileged. Doesn't that suggest you already haven't protected it enough? But note how weak the "shall consult as appropriate"

language is.

(12) Most of the Attorney Client language is redacted, but it seems they primary focus on stuff targeted at that person, and not necessarily other data.

(13) It's very clear, however, that the FBI permits itself to listen to protected communications, even those who have been charged locally.

(16) It appears NSA has a fairly persistent post-tasking problem determining location (is this just upstream collection?). I wonder if this passage was a response to the 2012 IG Report.

(17) Paragraph 3 affirmatively ensures that USP identities must "are accessible when a search or query is conducted or made of FISA-acquired information." I'm curious how this works, above, when some of this might not show up in queries. I'm just as interested by the "when a search or query is conducted or made." Why use this construction? Does this suggest something about searches that are substantively different than queries?

(17) Who all is included in those working at "others working at [prosecutors] discretion"?

(19) Prosecutors can access raw FISA data with Assistant Director approval.

(20) FBI has a retention exemption of metadata:

> The FBI is authorized to retain data in electronic and data storage systems other than those solely used for link analysis of metadata…

(20) FBI can retain data it has never reviewed longer than 5 years if they say it contains "significant foreign intelligence information."

(20) Even after deciding information is not FI, it will be retained for an additional period after the certification used to collect it

expires. Apparently, if that data responds to a search, the searcher must get approval from the Assistant Director or that person's designee to gain full access to this info. What officially counts as the expiration date, I'm not sure. Note that if this is held in an ad hoc database, it gets destroyed 5 years after the expiration of the cert.

(24) Does paragraph 2 say this doesn't get audited as closely as more established databases?

(24) Of course there's the indefinite decryption provision (though it is triggered to when the data is "subject to cryptanalysis."

(25) Interesting redaction of FBI's analytical techniques. Does that hide that FBI is permitted more pattern analysis than NSA, which is supposed to be limited for some of this to link analysis?

(28) FBI makes a dissemination distinction between foreign intelligence info (related to a threat), which can include USP data, and foreign power intelligence (not), which can only include USP data if necessary.

(28) This section does not list the crimes that Bob Litt listed (except for child porn).

(29) Go back and compare foreign govt redactions with 2006 SMPs.

(30) Why doesn't FBI have to report foreign disseminations to foreign govts?

(32) I think the NCTC language is designed to hand entire investigative files over (by case type — so presumably using a terrorism designation). This would seem to include significant tangential data. Also, is this limited to foreign terrorism?

(33) I believe the language in the computer intrusion dissemination is more lenient than language on info sharing.

(33) The serious harm designation matches NSA's,

in that it permits serious harm to property.

(21) Note how the original copy gets saved for 5 years but then can still be granted on a case-by-case basis. How?

(21) Paragraph 3 doesn't say it, but the "any other form" must be the 20/30 year retention practices.

(22) Retention for time outside of retention limits for litigation reasons must be documented. Where? Is it kept with the investigative file? Would defense attorneys ever learn of it?

(23) The ad hoc section repeats the "unconsenting" language, again raising questions of whether they're making a Third Party doctrine argument.

(##) A general comment. Other SMPs state very clearly what they mean by "US person identity" (these focus only on USP). We know from Section 215 discussions that FBI fights for very liberal definitions of what counts as an identifier (presumably not counting a unique email or phone number). So presume that applies here as well.